

Method and Apparatus for Random Bit-String Generation Utilizing Environment Sensors**ABSTRACT**

A random number generator that generates random numbers based on measurements of one or more environmental quantities. The random number generator includes a first sensor for generating a first sequence of digital values representing measurements of a first environmental quantity at successive times. A first compressor that provides a first sequence of compressed values having a lower internal correlation than the values of the first sequence of digital values compresses the sequence of digital values. The random number generator generates an output random number via a circuit for generating a random number from an input sequence of digital values, the input sequence being a function of one of the first sequence of compressed values. The circuit may utilize a hash function to provide further security. In addition, the circuit includes a blocking circuit for preventing the generator from outputting a random number if the input sequences fail a predetermined test.